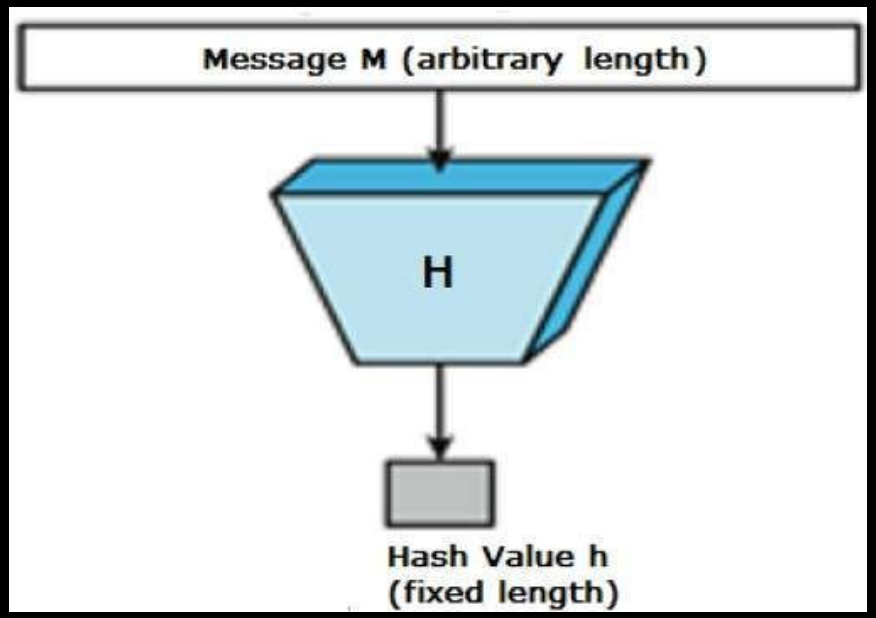
인공지능 보안

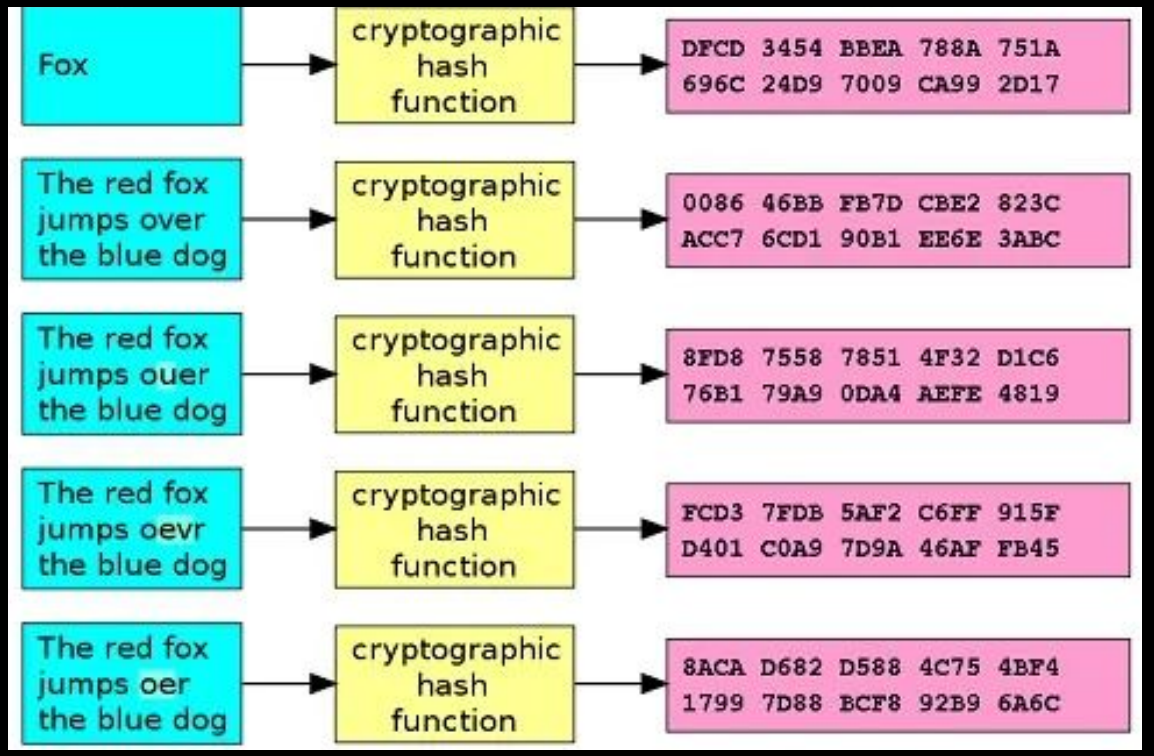
-08-

네트워크 보안

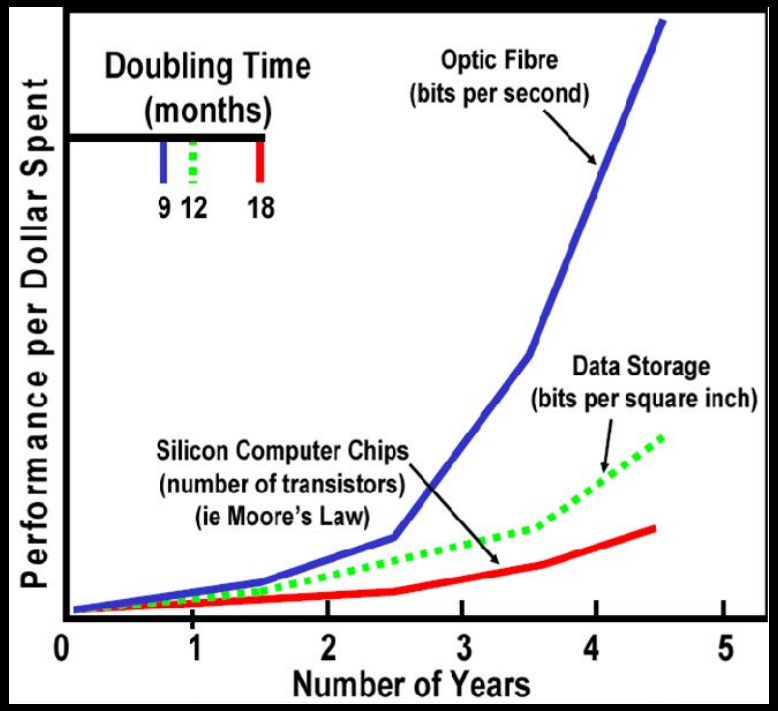
Hash

Hash Function



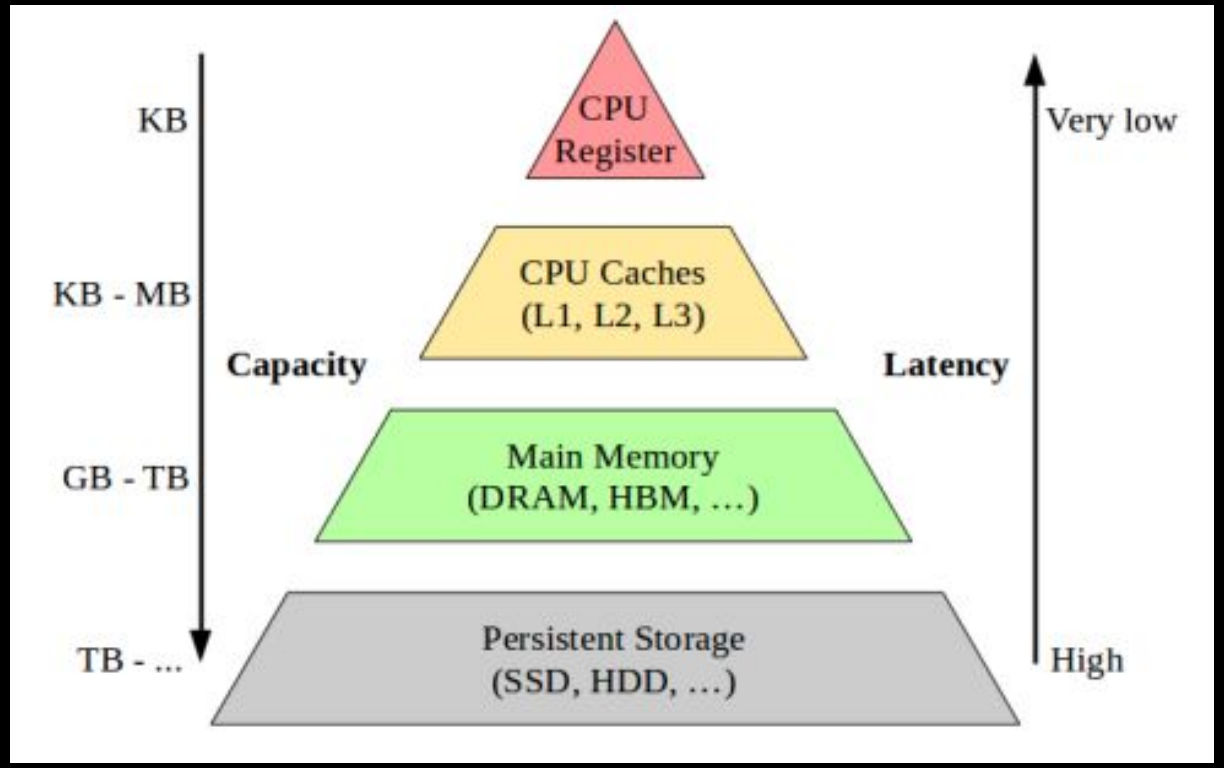


Security in High-speed Networks

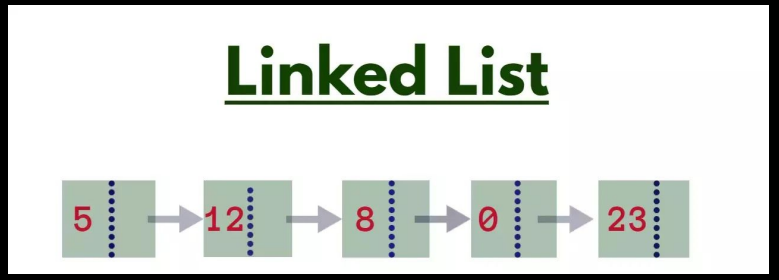


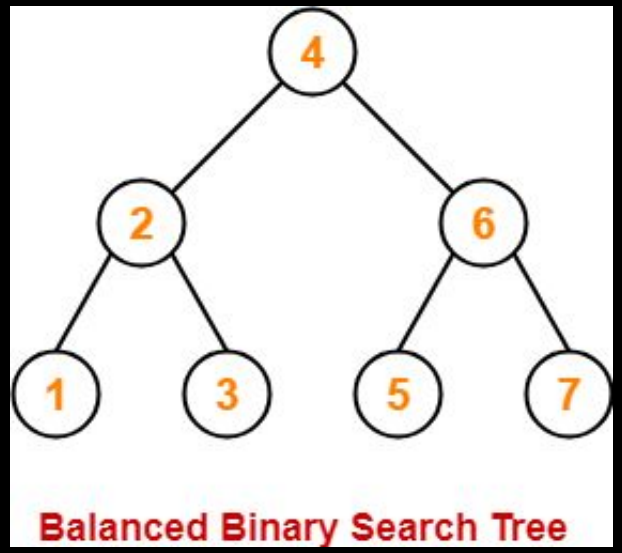
Moore's law comparison between the increase expectations of the network bandwidth and storage capacity

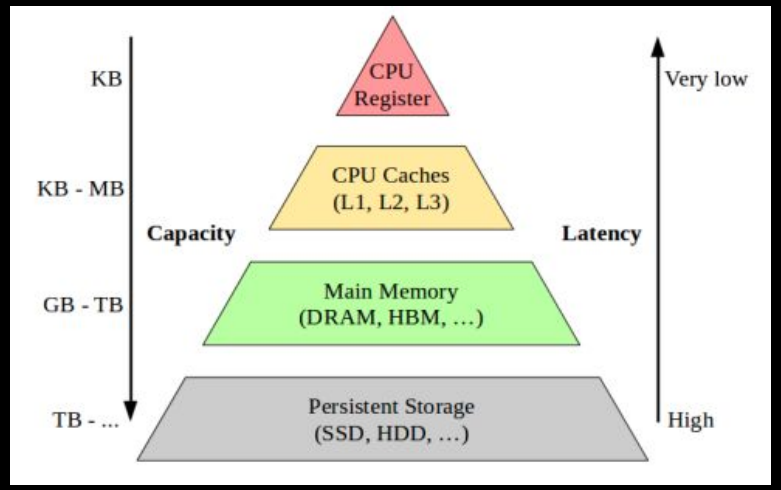
Memory Hierarchy



Complexity


Linked List
5
12
8
0
23

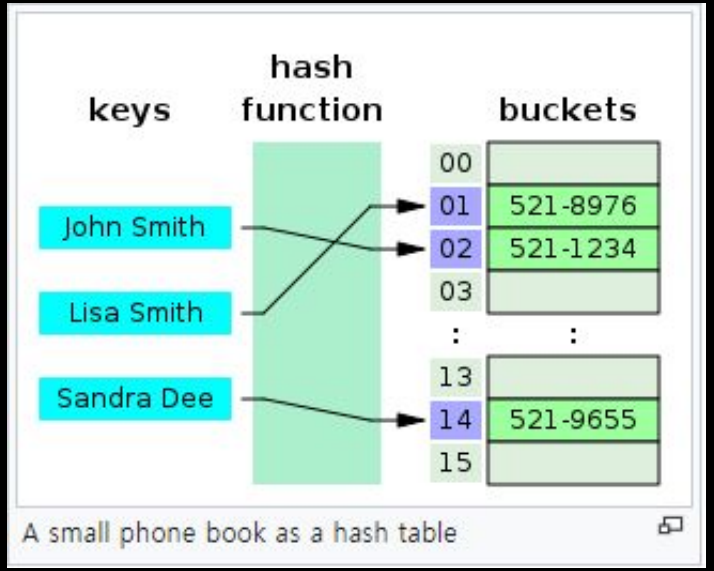

4
2
6
1
3
5
7
Balanced Binary Search Tree


KB
KB - MB
GB - TB
TB - ...
Capacity
CPU Register
CPU Caches (L1, L2, L3)
Main Memory (DRAM, HBM, …)
Persistent Storage (SSD, HDD, …)
Latency
Very low
High

Hash Table

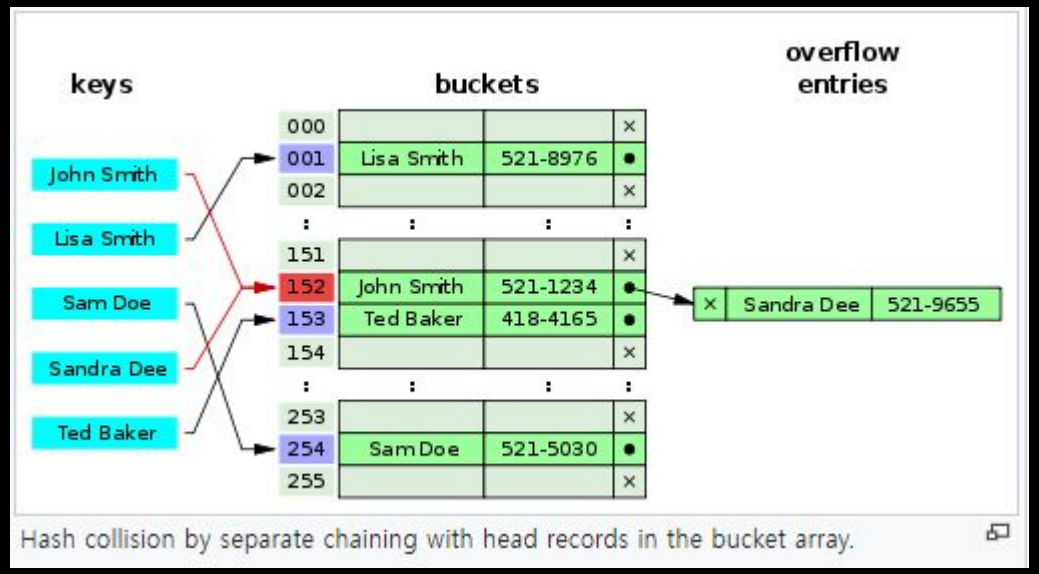
- The advantage of using hashing is that the table address of a record can be directly computed from the key

- Hash functions should provide a uniform distribution of hash values
- Cryptographic hash functions are believed to provide good hash functions for any table size, either by modulo reduction or by bit masking



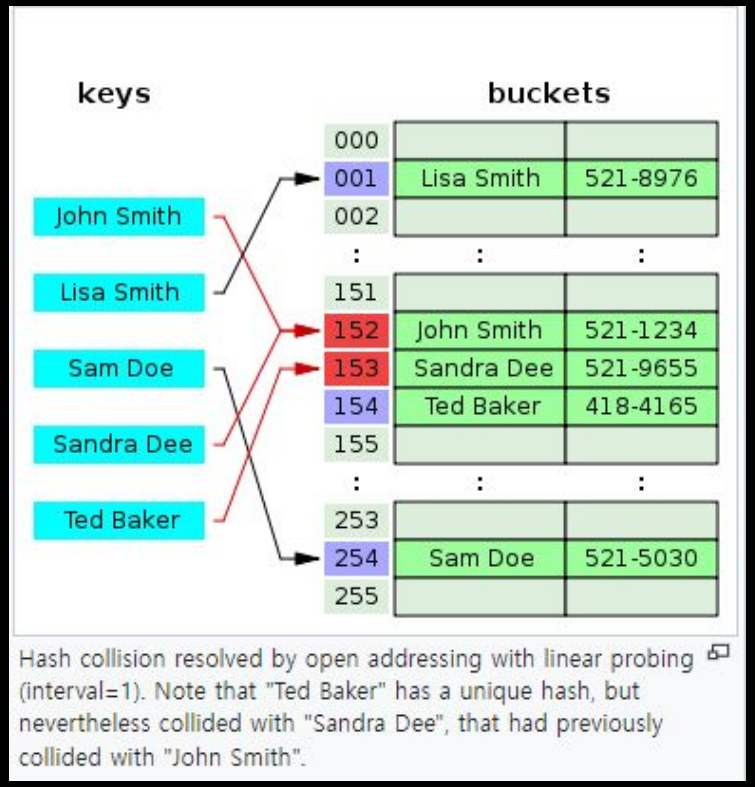
$$\text{Hash} = \text{Hash-Function(Key)}$$
$$\text{Index} = \text{Hash} \ \% \ \text{Hash-Table-Size}$$

Hash Table



Hash collision by separate chaining with head records in the bucket array.

Chaining

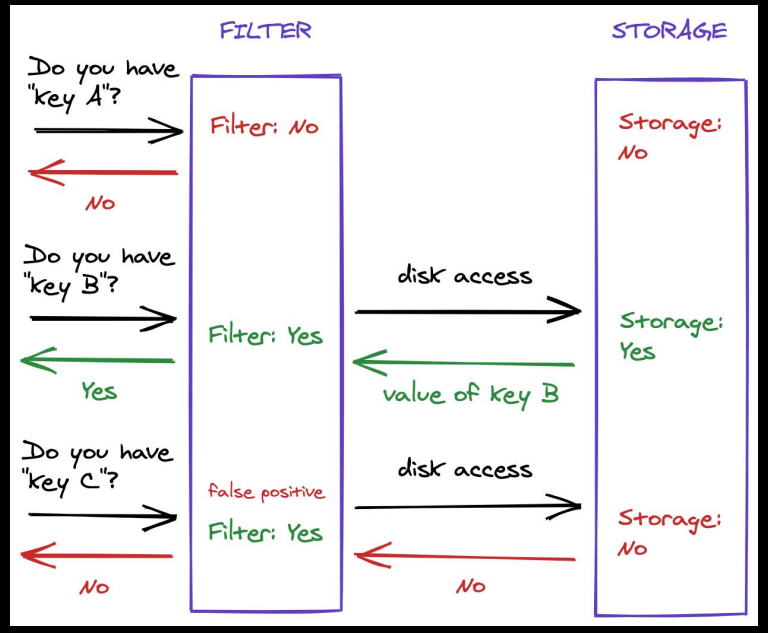


Hash collision resolved by open addressing with linear probing (interval=1). Note that "Ted Baker" has a unique hash, but nevertheless collided with "Sandra Dee", that had previously collided with "John Smith".

Open addressing

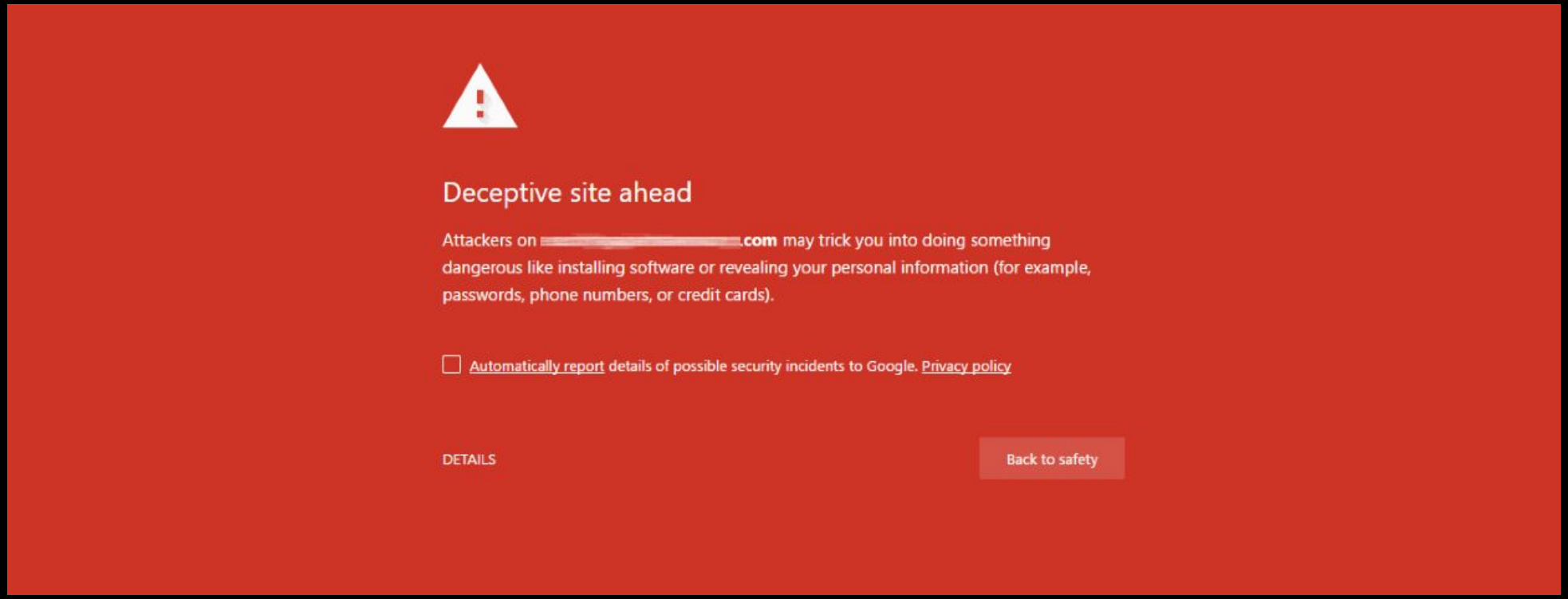
Bloom Filter

Bloom Filter



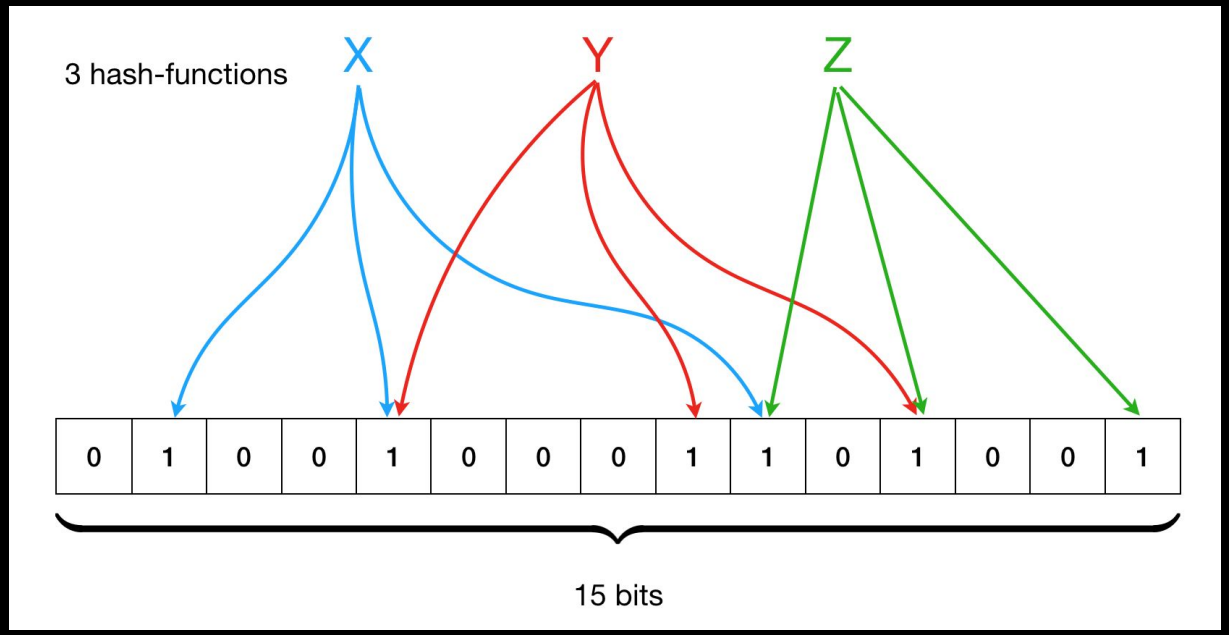
A space-efficient probabilistic data structure that is used to test whether an element is a member of a set.
False positive matches are possible, but false negatives are not - in other words, a query returns either "possibly in set" or "definitely not in set".

Bloom Filter



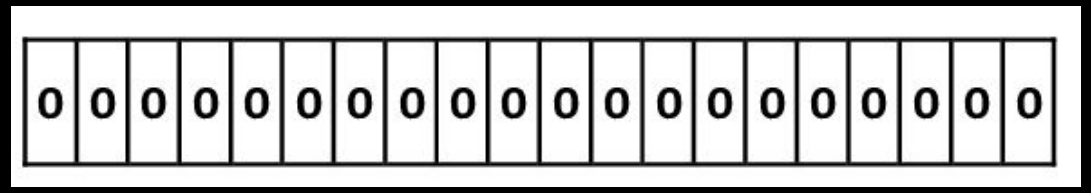
Google Chrome warning user when the user visits a malicious website

Bloom Filter

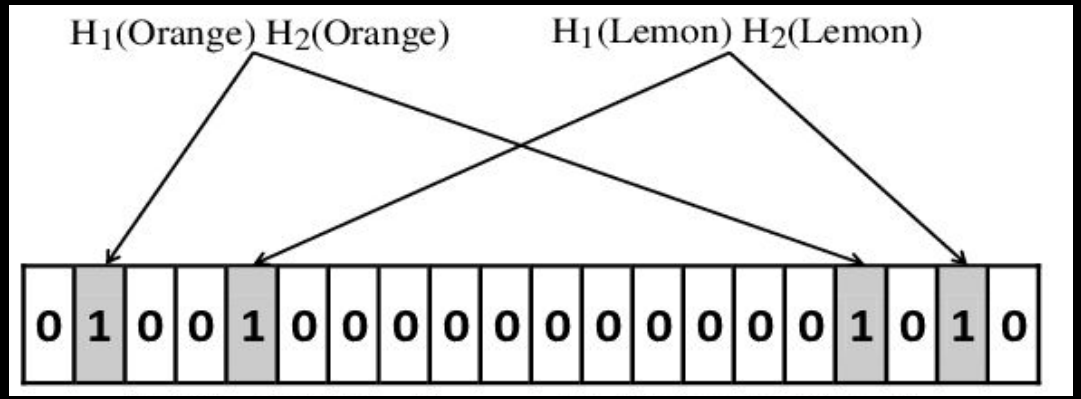


bit array of size m(15)
k(3) of different hash-functions

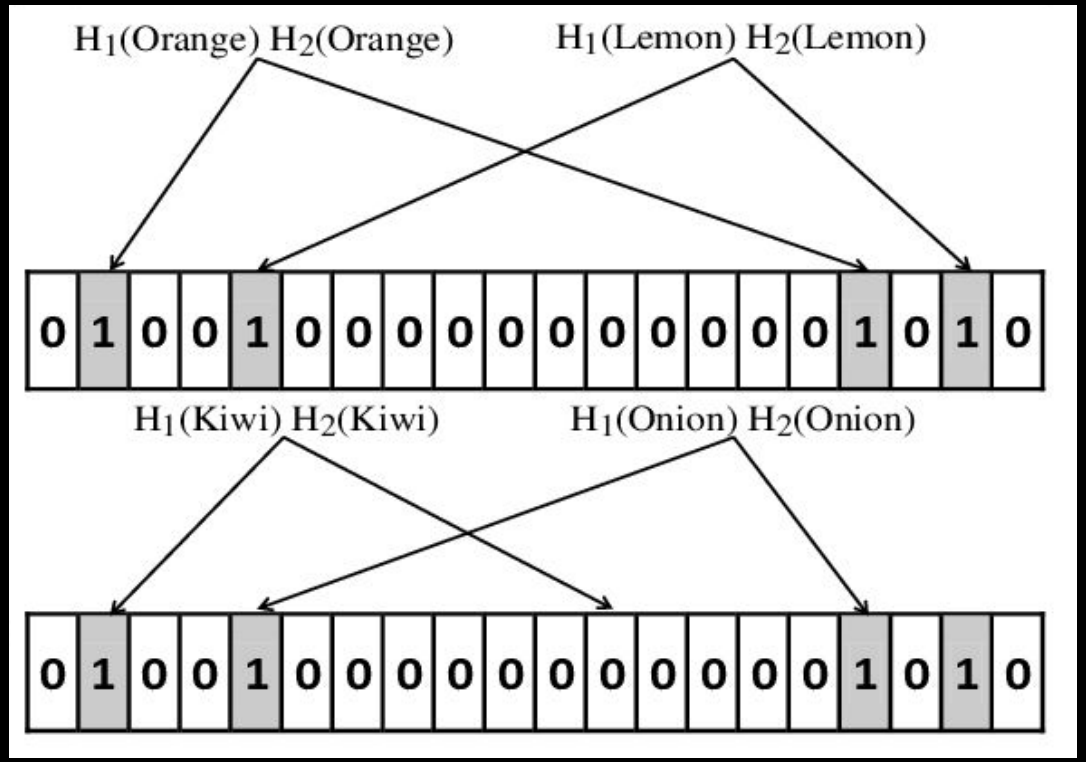
Bloom Filter : Initialize



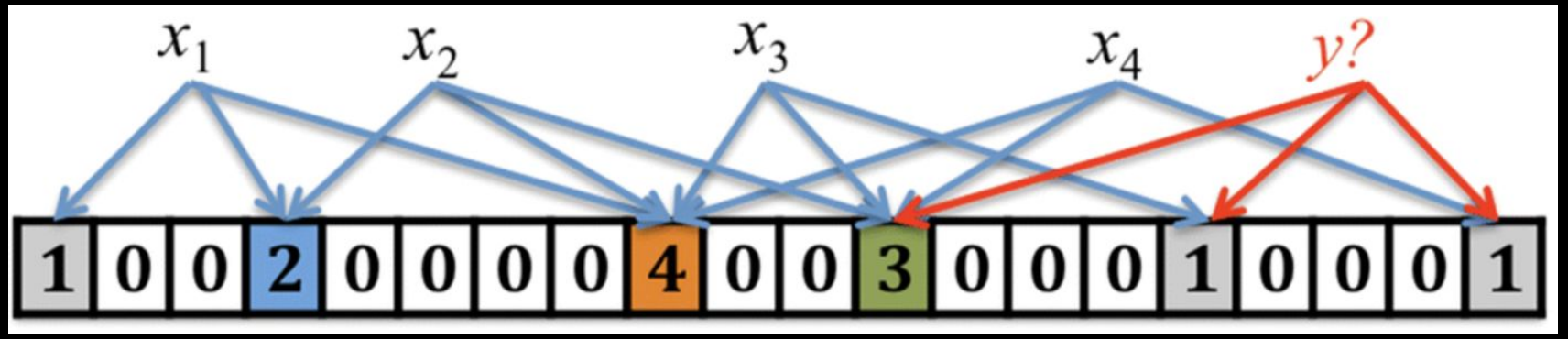
Bloom Filter : Insert



Bloom Filter : Query



Counting Bloom Filter



Q&A